IT Unit 3

Topic 1

# Organisations & Data Management

**Protecting valuable data, p 57**

1. Why is it important that stored data is kept secure?

Data is kept secure to hold integrity and to maintain the most accurate data possible, it also ensures that no confidential is leaked from the system, to be up to privacy legislations, to maintain in a good business reputation.

1. What are the 2 types of controls that can protect data?

Physical and software based controls can be used to protect data with physical be restricting access to the site or protection for the weather or other natural disasters as software base protection restricts access to the information like a firewall to stop hackers

Measures to protect data:

Physical equipment controls include zoned security strategies, barrier techniques and biometrics.

A What is meant by biometrics and what is its advantage as a means of protecting data?

1. Backing up
   1. What are the 3 types of backing up?

Full (A backup of all files on 2 or more media), Differential (backs up all data changed since the last full back up on 2 or more media) or incremental (backs up all data changed since the last back up on 2 or more media)

* 1. List some backup options?

Version control allows a Database to roll back to the last version in case something becomes corrupted or worse.

1. Electrical protection
   1. What is the role of a UPS?

An UPS (uninterruptable power supply) can regulate electricity coming into a computer and supply backup electricity for a short time if a black out occurs.

1. Usernames & passwords
   1. What are the characteristics of a good password?

A good password is made up of a number of different characteristics. For instance, it should be at least 6 - 8 characters long and should include at least two uppercase letters, lowercase letters and numbers.

* 1. What is the role of access logs, audit trails and access restrictions?

These are restrictions that a company can employ in their websites and to see places that users have accessed during their time on the site.

1. Systems security software
   1. What types of security software should organisations run?

Firewalls are used to prevent unauthorised users from accessing data or doing with unauthorised or harmful things to the data.

* 1. Explain the nature of malware and phishing software

There are various types of malware and phishing software but all usually tries to either obtain sensitive data from one’s system or to disrupt operation.

* 1. Explain the nature of a firewall?

A firewall is a type of filter that is found between the system and the world-wide web and filters data incoming and outgoing to stop anything that is deemed malicious from passing through, and is also used to restrict users access to a certain network.

1. Encryption
   1. What does encryption involve?

Encryption is used to prevent interception and theft by creating a primary key which is then used to change the data of the files to make them unreadable

* 1. What protocols are used for encryption?

Encryption uses SSL or TLS to create a secure HTTP connection (HTTPS)

* 1. What is hashing?

When stored, databases can also be encrypted. The contents can be encrypted inside fields. This is known as hashing and is often used to protect passwords. The entire database file can also be encrypted so that, if stolen, its contents cannot be opened and used by another person.